UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/522,472	02/06/2006	Jan Camenisch	CH920020013US1	3674

877 7590 12/15/2008

IBM CORPORATION, T.J. WATSON RESEARCH CENTER
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/522,472	CAMENISCH ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 4-6, 13, 16, and 17 are rejected under 35 U.S.C. 102(e) as being anticipated by Hopkins et al. (US Patent Publication No. 20030120931 and Hopkins hereinafter).

3. As to claim 4, Hopkins teaches a method comprising providing a signature value on a message in a network of connected computer nodes (i.e., … teaches distributing individual private keys to a plurality of authorized individuals each of whom may then sign a message using his or her associated individual private key to create an associated partial digital signature [par. 30]), the method being executable by a first computer node and the step of providing comprising the steps of:

- selecting a first signature element (i.e., prime factor) from a plurality of signature elements (e.g., a collective group of prime factors) comprising said signature (e.g., signing a message) (i.e., … teaches a signing process using the group private key D wherein each of the members of each group has control over at least one of the prime factors p.sub.1, p.sub.2, . . .

p.sub.k, and wherein each group of individuals collectively has control of all of the prime factors p.sub.1, p.sub.2, . . . p.sub.k, but wherein no single one of the individuals of the group controls all of the prime factors used by the entity [par. 67]);

- selecting a signature exponent value from a number of exponent values, said signature comprised of a plurality of signature exponent values (i.e., …teaches an associated individual private exponent d.sub.i that is determined based on a selected public group exponent e [claim 3]);

and - deriving a second signature element from a provided secret cryptographic key (i.e., … teaches deriving a hash value of the message to be signed and then performing a mathematical operation on that value using the private key [par. 9]), the message, and the number of exponent values such that the first signature element, the second signature element and the signature exponent value satisfy a known relationship with the message and a provided public cryptographic key (i.e., …teaches messages associated with an entity represented by the group, and the prime numbers p.sub.1, p.sub.2, . . . p.sub.k are referred to as factors of the group modulus n. As mentioned, the prime numbers p.sub.1, p.sub.2, . . . p.sub.k satisfy the criteria of being distinct, random, and suitable in accordance with relationships (2) through (6), above. The private key D, defined in accordance with relationship (7) above, which includes the composite number n and the private exponent d [par. 66]),

wherein the signature value comprises the first signature element, the second signature element, and a signature reference to the signature exponent value (i.e., … teaches sub-tasks are then solved to determine results S.sub.1, S.sub.2 . . . S.sub.z which are subsequently combined in accordance with a combining process to produce the signature S [par. 59] … further teaches digital signatures are generated by each individual at a corresponding one of the

individual systems 16 (FIG. 1) based on the associated individual cryptosystem defined by the associated individual modulus n.sub.IND and the associated individual private key exponent d.sub.IND [par. 78]), the signature value being sendable within the network to a second computer node for verification (i.e., …teaches the digital signature is attached to the corresponding message and transmitted to a second party [par. 9]).

4. As to claim 5, Hopkins teaches a method where the step of deriving a second signature element further comprises deriving a signature base value using a provided public cryptographic key, the provided secret cryptographic key, and the exponent values (i.e., …teaches digital signatures are generated by each individual at a corresponding one of the individual systems 16 (FIG. 1) based on the associated individual cryptosystem defined by the associated individual modulus n.sub.IND and the associated individual private key exponent d.sub.IND [par. 78]).

5. As to claim 6, Hopkins teaches a method further comprising deriving a previously presented secret cryptographic key from the provided secret cryptographic key and the selected signature exponent value (i.e., … teaches the first individual private key includes: an associated individual modulus n.sub.1 that is determined as the product of a number m.sub.1 of distinct prime factors of the group modulus n; and an associated individual private exponent d.sub.1 that is determined based on a selected public key exponent e and based on the m.sub.1 prime factors of the associated individual modulus in accordance with 1 d 1 e - 1 mod (j m 1 (p j 1) [par. 19]).

6. As to claim 13, Hopkins teaches a method further comprising applying each of the exponent values to at most one signature value [par. 57].

7. As to claim 16, Hopkins teaches a computer program element comprising program code means for performing the method of claim 4, when said program is run on a computer [par. 39].

8. As to claim 17, Hopkins teaches a computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 4 [par. 39].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 1-3, 9-12, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schweitzer et al. (US Patent No. 5,850,450 and Schweitzer hereinafter) in view of Hopkins.

10. As to claim 1, Schweitzer teaches a method comprising providing a secret cryptographic key and a public cryptographic key applicable in a network of connected computer nodes using a signature scheme (i.e., …teaches generating a two-key encryption key set comprising a private component and a public component [claim 5]), the method being executable by a first computer node and the step of providing comprising the steps of:

- generating the secret cryptographic key by - selecting two random factor values (i.e., ...teaches generating a first random prime number; generating a second random prime number [claim 5]) ,

- multiplying the two selected random factor values to obtain a modulus value (i.e., …teaches producing a modulus by multiplying said first random number by said second random prime number [claim 5]), and

- selecting a secret base value (i.e., prime number) in dependence on the modulus value, wherein the secret base value forms part of the secret cryptographic key (i.e., ...teaches generating a first and second key based on said first and second prime numbers [claim 8]);

- deleting the two random factor values (i.e., …teaches first and second random prime numbers is obtained by concatenating a first and second plurality of random bytes, respectively, and further wherein the contents of said random bytes are associated with a random event the use of random number [claim 5]. Examiner contend the fact that the number are random inherently teaches they will be deleted automatically);

Schweitzer does not teach:

- providing the public cryptographic key within the network;

- generating the public cryptographic key by - selecting a number of exponent values, and deriving a public base value from the exponent values and the secret base value, wherein the public base value and the modulus value form part of the public cryptographic key

such that the public cryptographic key and at least one of the selected exponent values is usable for verifying a signature value on a message to be sent within the network to a second computer node for verification.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schweitzer as introduced by Hopkins. Hopkins discloses:

- providing the public cryptographic key within the network (to provide the cryptographic key within the network [fig. 1] ;

- generating the public cryptographic key by - selecting a number of exponent values, and deriving a public base value from the exponent values and the secret base value, wherein the public base value and the modulus value form part of the public cryptographic key (for purpose of generating a cryptographic key Hopkins provides for the an associated individual modulus n.sub.i that is a number formed as a product of one or more of the k prime factors of the group modulus n such that an associated individual private exponent d.sub.i is determined based on a selected public group exponent e, and also based on the prime factors of the associated individual modulus n.sub.i. Hopkin further provide for each of the individual private exponents

d.sub.i may be determined as a number congruent to the inverse of the public group exponent e, modulo the Euler Totient function of the associated individual modulus n.sub.i [par. 18]).

such that the public cryptographic key and at least one of the selected exponent values is usable for verifying a signature value on a message to be sent within the network to a second computer node for verification (for purpose of verifying a signature value Hopkins provides to verify the signed message M would of course need to know the public key including modulus n and the public exponent e in order to compute h(M)'.. [par. 57]);

Therefore, given the teachings of Hopkins, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schweitzer by employing the well known features of using a public key and exponent values to verifying a signature value of a message disclosed above by Hopkins, for which signature security will be enhanced [par. 57]).

11. As to claim 2, Schweitzer teaches a method further comprising providing a description of the exponent values within the network (i.e., ...teaches D is the private exponent and E is the public exponent, then the "encryption" key set comprises [E;N], whereas the "decryption" key set comprises [D;N]. The host 10 can send an encrypted message to the electronic data module 100 (shown in FIG. 1) having the decryption key, D, stored internally thereto, by computing M.sup.E Mod N, where M denotes the plaintext. The data module 100, upon receiving the ciphertext, C, can decrypt by computing C.sup.D Mod N using the stored decryption key, D [col. 15, lines 20-35]).

12. As to claim 3 and 9, the system disclose by Schwitzer teaches substantial features of the claim invention (discussed above) it fails to disclose:

A method further comprising defining an order of the selected exponent values for enabling to communicate the validity of the signature value in the event of a detected intrusion (claim 3).

A method further comprising applying each of the exponent values to at most one signature value (claim 9).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schweitzer as introduced by Hopkins. Hopkins discloses:

A method further comprising defining an order of the selected exponent values for enabling to communicate the validity of the signature value in the event of a detected intrusion (claim 3) (to define a exponent order for purpose of signature verification [par. 57]).

A method further comprising applying each of the exponent values to at most one signature value (claim 9) (to apply a exponent value for verification of a signature [par. 57]).

Therefore, given the teachings of Hopkins, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schweitzer by

employing the well known features of using exponent values to verifying a signature value of a message disclosed above by Hopkins, for which signature security will be enhanced [par. 57]).

13. As to claim 10, Schweitzer teaches a computer program (i.e., processor instruction performed by processor) element comprising program code means for performing the method of claim 1 when said program is run on a computer [20, fig. 1].

14. As to claim 11, Schweitzer teaches a computer program product stored (i.e., processor instructions) on a computer usable medium, comprising computer readable program means for causing a computer to perform the method according to claim 1 [20, fig. 1].

15. As to claim 12, Schweitzer teaches a network device comprising: - a computer program product (i.e., processor instructions); - a processor for executing the method; - the processor having access to exchanged messages in the network [20, fig. 1].

16. As to claim 22, Schweitzer teaches a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing functions of a network device [20, fig. 1], the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 12 [20, fig. 1].

17. Claims 7, 14, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins.

18. As to claim 7, Hopkins teaches a method comprising verifying a signature value on a message in a network of connected computer nodes (i.e., … teaches a verifying a signature on a message [par. 94]), the method being executable by a second computer node and the step of verifying comprising the steps of:

- receiving the signature value from a first computer node the digital signature is attached to the corresponding message and transmitted to a second party. Verification of the digital signature is accomplished by computing a new hash result of the original message using the same hash function that was used to create the digital signature. Using the public key to invert the received signature [par. 9]);

- deriving a signature exponent value from the signature value (i.e., …teaches A verification process of the Multi-Prime signature scheme provides for converting the signature S to a candidate hash h(M)' using the public exponent e as a verification exponent [par. 56]);

and - verifying whether the signature exponent value and part of the signature value satisfy a known relationship with the message and a provided public cryptographic key (i.e., …teaches to verify the signed message M would of course need to know the public key including modulus n and the public exponent e in order to compute h(M)'. After computing h(M)', if it is determined that h(M)=h(M)', the signature would be verified as originating from the entity associated with the public exponent e and the modulus n [par. 57]), otherwise refusing the signature value, wherein the signature value was generated from a first signature element, a number of exponent values, a provided secret cryptographic key, and the message.

Hopkins does not teach:

otherwise refusing the signature

However the claim feature of "otherwise refusing the signature" upon unsuccessful signature verification is well known in the art and would have been an obvious modification of the system disclosed by Hopkins. Therefore, given the teachings of Hopkins, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage to refuse the signature based on a unsuccessful signature verification for which signature security would be enhanced.

19. As to claim 14 Hopkins teaches a method further comprising applying each of the exponent values to at most one signature value [par. 57].

20. As to claim 18 Hopkins teaches a computer program element comprising program code means for performing the method of claim 7, when said program is run on a computer [par. 39].

21. As to claim 19 Hopkins teaches a computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 7 [par. 39].

22. Claims 8, 15, 20, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins in view of Johnson (US Patent Publication No. 2001/0014153), further in view of Staddon et al. (US Patent Publication No. 20040017916 and Staddon hereinafter).

23. As to claim 8, Hopkins teaches a method comprising communicating within a network of connected computer nodes the validity of a signature value in the event of an exposure of a secret cryptographic key relating to the signature value (i.e., … teaches a verifying a signature on a message [par. 94]), the step of communicating comprising the steps of:

defining an order of exponent values [par. 57];

and a provided public cryptographic key [fig. 1],

Hopkins does not teach;

order of exponent values,

publishing a description of the exponent values and the order of the exponent values within the network ;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Hopkins as introduced by Johnson. Johnson discloses:

order of exponent values (to provide the capability to order exponents [par. 20]).

publishing a description of the exponent values and the order of the exponent values within the network (to publish exponent value for purpose of validating signature [par. 21, lines 10-14]);

Therefore, given the teachings of Johnson, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Hopkins by

employing the well known features exponent value ordering disclosed above by Johnson, for which signature validation will be enhanced [par. 21, lines 10-14].

The system disclose by Hopkins in view of Johnson teaches substantial features of the claim invention (discussed above) it fails to disclose:

publishing a revocation reference to one of the exponent values within the network such that the validity of the signature value is determinable by using the revocation reference

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Hopkins in view of Johnson as introduced by Staddon. Staddon discloses:

publishing a revocation reference (i.e., revoke user are made public) to one of the exponent values within the network such that the validity of the signature value is determinable by using the revocation reference (to provide revocation notification of revoked parameters [par. 117, lines 4-8]).

Therefore, given the teachings of Staddon, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Hopkins in view of Johnson by employing the well known features of revocation notification disclosed above by Staddon, for which signature validation will be enhanced par. 117, lines 4-8].

24. As to claim 15, Hopkins teaches a method further comprising applying each of the exponent values to at most one signature value [par. 57]

25. As to claim 20, Hopkins teaches computer program element comprising program code means for performing the method of claim 8, when said program is run on a computer [par. 39].

26. As to claim 21, Hopkins teaches a computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 8 [par. 39].

Response to Arguments

Applicant's arguments, see Amendment/Req. Reconsideration, filed 8/27/2008, with respect to the rejection(s) of claim(s) 1-22 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Hopkins et al. (US Patent Publication No. 20030120931).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435